STRATEGY RESEARCH PROJECT

THE IMPACT OF COMPUTER NETWORK ATTACKS ON INFRASTRUCTURE CENTERS OF GRAVITY

BY

LIEUTENANT COLONEL ALLAN D. PAYNE
United States Air Force Reserve

USAWC CLASS OF 1999

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

The Impact of Computer Network Attacks on Infrastructure Centers of Gravity

by

Lt Col Allan D. Payne
USAFR

Professor Robert F. Minehart, Jr.
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Allan D. Payne, Lt Col, USAFR

TITLE: THE IMPACT OF COMPUTER NETWORK ATTACKS ON INFRASTRUCTURE CENTERS OF GRAVITY

FORMAT: Strategy Research Project

DATE: 7 April 1999 PAGES: 24 CLASSIFICATION: Unclassified

Computer Network Attack is a significant asymmetric threat to the United States and its military. Motives vary, but the threat from CNA is real; US infrastructure targets are vulnerable; those that directly affect the ability of the US military to conduct its missions are evident. Innovation in CNA is unrestrained, and privacy rights of the US citizenry conflict directly with US government efforts to take active measures to help defend against CNA. CNA today could be economically damaging to the computer and network dependent society that the United States has become. The challenge is to define the problem separately from every other consideration and challenge that the military faces in the Information Age including the broader mission areas of Information Operations and Information Warfare.

TABLE OF CONTENTS

LIST OF TABLES

LONDON Sunday February 28, 1999 - Hackers have seized control of one of Britain's military communication satellites and issued blackmail threats, The Sunday (Reuters) Business newspaper reported. The newspaper, quoting security sources, said the intruders altered the course of one of Britain's four satellites that are used by defense planners and military forces around the world... ``This is a nightmare scenario,'' said one intelligence source. Military strategists said that if Britain were to come under nuclear attack, an aggressor would first interfere with military communications systems.

-- Reuters[1]

THE IMPACT OF COMPUTER NETWORK ATTACKS ON INFRASTRUCTURE CENTERS OF GRAVITY

Throughout January, members of the Army War College Class of '99 were able to ask probing questions of several senior leaders in the US Defense establishment regarding Information Operations. The leaders included strategic leaders and visionaries from the US Intelligence Community, two CINCs as well as the most senior leaders at the War College[2]. The opinions of these leaders were varied and thought provoking. Although comments are privileged and anonymous due to a policy of non-attribution, one senior leader, who should be described as a local senior theorist regarding the future conduct of our wars, discounted the potential threat of information or network-based attacks upon the critical infrastructure of the United States. He argued that any threatening state would be foolish to take on the US, and its powerful will on its home territory via any type of provable disruption to its way of life. Others described and even demonstrated the effects of what is termed a "Computer Network Attack", or CNA, how it could disrupt and how easy it was to undertake such an intrusion into a network. The purpose of this paper is to position such a potential threat to the United States and its military, what the likely motives would be and then assess the current defense posture of the United States in light of the civil political considerations and whether the US government is adequately covering all of the CNA threats. The threat from CNA is real; US infrastructure targets are vulnerable; innovation in CNA

is unrestrained, and privacy rights of the US citizenry conflict directly with US government efforts to take active efforts to help defend against CNA. CNA today could be economically damaging to the computer and network dependent society that the United States has become. The basic threat question is could CNA provide a significant blow to American responsiveness to a major international crisis or a major regional crisis contingency that affects vital national interests? The answer is not yet clear, yet there are indications, because the attacks would be organized and synchronized that it could be much more threatening than the looming Y2K problem. A concerted, coordinated and focused attack against the networks and computer systems of United States, including its civilian economic and monetary systems and power or telecommunications infrastructure would be devastating. What would an adversary achieve? What would be the motivation or motive of an adversary state? The easy answer is that an adversary could easily achieve the ends of economic chaos in the United States, at least on a temporary basis and possibly for a longer term impact affecting American financial institutions, telecommunications, transportation and power system reliability. The CNA threat needs to be addressed in terms of what efforts the United States defense establishment should take to ensure its relative protection from CNA attack. Do the specific efforts and actions require that citizens give up its expectation of privacy in its communications?

THREATS AND DEFINITIONS

THE THREAT OF INFORMATION WARFARE AND OPERATIONS

On June 10th of 1998, Senator Jon Kyl (Republican from Arizona) reported that the National Security Agency briefed his Senate Judiciary Subcommittee on Terrorism and Technology. Senator Kyl stated that concurrent with the tensions in the Gulf this past February, which resulted in the significant US military build-up there, hackers broke into US military computers and eluded identification for four days in an incident the government termed "Solar Sunrise"[3]. Senator Kyl states that this was significant because "For four days, our government

did not know who was attacking key defense computers essential to deploying forces to the Persian Gulf. Fortunately, this time, the hackers were teenagers, not Iraqi forces. But what about next time?"[4] The subsequent arrest of the teens connected them with a mentor and advisor who not only represented a foreign nation but was also located halfway around the world when providing advice and mentorship. The entire Solar Sunrise experience validated not only that the "information security" or "information defense" part of information operations was vital to our security, but also that CNA, computer network attack, as "information operations" was also possible. Unfortunately, "information warfare" or "information operations" as addressed by the US Department of Defense, has previously included not only these types of attacks, but instead operates in a realm including most everything that is digital, sensor, robotic, intelligent or happens to be computerized or communicated electronically. Indeed, making all things "information" into a "revolution in military affairs" or "RMA" by glorifying this "Third Wave", the effect could be to so overwhelm the nation, defense establishment and complicate this so much as to ignore the potential threat that real "computer-communications" weapons or hacker weaponry can have on our national and military "centers of gravity". These could include US domestic information "centers of gravity" such as infrastructure susceptible to what has generally been described as an "electronic Pearl Harbor". Secretary of Defense Cohen's "Report of the Quadrennial Defense Review" states clearly the priorities for implementing the DoD "Joint Vision 2010", a blueprint for operations and strategy in the year 2010, by emphasizing that information superiority is a true RMA that needs as a key element "an information operations capability able to penetrate, manipulate, or deny an adversary's battlespace awareness or unimpeded use of his own forces..."[5] The spectrum of war operations in the "Third Wave World" described by Alvin and Heidi Toffler[6] presents an overwhelming array of everything from PGMs (precision guided munitions) to space to robots to information economic terrorism. In addition, the future can be analyzed in terms of an explosion of "Extraordinary Technology"[7] that most directly affects not only our information society but also the means that we might use to conduct "information warfare" or as described now by the Pentagon, "information operations", both offensive and defensive. Indeed, by the year 2010

"information" will become a part of everything the US military does, as a matter of doctrine. Such current "2010" strategies as "infospace dominance", the "digital battlefield" and "information superiority" are really only updated terms for high-tech command and control, electronic indications and warning ("I&W"), real-time intelligence and reconnaissance and the communications security ("COMSEC") and operations security ("OPSEC") to protect all of these from a potential adversary.

The current National Security Strategy regarding information operations is new although the defensive and offensive aspects of communications security date from the early days of war, intelligence and espionage, perhaps even from the days of Sun Tzu[8]. Interestingly, the most recent White House security strategy "A National Security Strategy for a New Century" does describe a need to protect "information infrastructure"[9] as a major objective of national security.

Information operations per se has been defined as "actions taken across the entire conflict spectrum to affect adversary information and information systems while protecting one's own information and information systems."[10] This definition is a concise one only if US strategy and doctrine allows for offensive information operations to be integrated with any operational campaign and defensive information operations to occupy a position equal and parallel with "operations security" during military campaigns. Since the spectrum of information operations can be so broad, the objectives or ends that can be attacked with its techniques, can be quite diverse, and can vary greatly in their results, destructiveness or even lethality. US defense strategy for defensive information operations while fairly well defined, is currently well dispersed throughout the federal government.

A single presidential initiative, the President's Commission on Critical Infrastructure Protection ("PCCIP"), has studied strategic defensive information operations in depth and specifically the defense against CNA, with the charter to report back to the administration and Congress on its findings. Its report was completed in October 1997. Its charter and its staff were temporary, and its report wide-ranging regarding the threat. Partially as a result, defense against CNA from external and internal threats are now a priority of the US Government with the

"Computer Enhancement Security Act of 1997, which continues to give the lead in this effort to the National Institute of Standards and Technology ("NIST").[11]

Just last week, Secretary of Defense Cohen briefed employees of the Microsoft Corporation in Redmond, Washington. In this extraordinary admission of the power of a private corporation to "shape" the defense of our nation, Mr. Cohen asked for Microsoft's cooperation in partnership to help ensure defense against potential CNA[12]:

> A year ago, during a tense build-up in the Persian Gulf, a cyber-attack on our systems exposed the extent of our vulnerability. No data was compromised, but it was the most serious and sustained attack ever against our information systems, and it was conducted by teenagers. Today, as you well know, small groups, even single individuals, can wage electronic war against the most powerful nation in the world using off the shelf, existing tools and technologies.
>
> We are taking this problem very seriously, continuing to build defenses against this threat. We have created a new Chief Information Officer for the department, who is reorganizing our strategies to better confront the danger. All together, the Department of Defense will spend $3.6 billion on computer security in the next four years. Our work is part of a larger government effort to keep our information-based economy safe from disruption. Our national infrastructure not only runs everything from air traffic control to financial transactions. It carries ninety-five percent of all Department of Defense communications, everything from satellite navigation, to command and control, to transportation.
>
> That is why the Administration is implementing a new presidential plan to build national information assurance measures, directed by a senior coordinator on the National Security Council. We have already created a National Infrastructure Protection Center at the FBI but, of course, we cannot hope to solve these problems without a partnership with your industry. Time and again, our national security has benefited when government and private organizations join hands to serve the public interest. Together we can insure that the technology, which has enabled leaps in productivity, does not endanger our prosperity.

THE TOO-BROAD DEFINITION OF INFORMATION WARFARE

As noted, Information Operations, or Information Warfare, can take many forms. Martin Libicki, of the National Defense University, defines the spectrum as being quite broad and diverse[13]. The Libicki topology has been referenced in various DoD analyses and includes the dimensions shown below. This topology presents a very complete spectrum of definitions that can include many aspects of information operations or information warfare.

Form	Description	Subtypes (Weapons Functionality)
C2W	Command & Control	Antihead & Antineck
IBW	Intel-based InfoWar	Targeting and Bomb Damage
EW	Electronic Warfare	Anti-radar-comms-cryptography
Psycho	Psychological War	Antiwill, Antitroop, Kulturkamp
Hacker	Hacker Warfare	CAN, Sabotage, Identity Fraud
Economic	Economic Info War	Techno-Imperialism
CyberWar	Cyber Warfare	Info-terrorism, Simulawarfare

Table 1-- The Spectrum of Information Operations[14]

The problem is that defining information warfare and information operations in these broad terms does little to focus defenses against current and new threats that take advantage of new weapons systems opportunities -- the threat and use of Computer Network Attacks ("CNA"). When the United States addresses certain "strategic" centers-of-gravity such as a country power grid, stock market or banking system, are you able to actually target centers-of-gravity that can approach strategic devastation. Due to the exceedingly large scope of information operations, there are diverse initiatives throughout the US Department of Defense. Mr. Robert Minehart, Professor at the Army War College, while acknowledging the broad definition of information warfare, more narrowly defines information operations weaponry in relatively specific CNA terms, akin to the "Hacker" forms of Mr. Libicki, above. Mr. Minehart covers information operation weapons with the various characteristics and speculates that information operations weaponry could be employed at various points on the "ends" spectrum -- at the strategic national, theater strategic, operational, or tactical levels[15]. Mr. Minehart's "weapons" and targets include hack attacks, malicious software, back doors, destructive microbes, attacks on the banking system, denial of service, and disruption of national systems such as the air traffic control system, power grid or telephone

systems, that could result in the "electronic Pearl Harbor" previously noted[16]. These could be the weapons of choice of an adversary state or adversary non-state actor that fit the scenario described here.

NETWORK STRATEGIC CENTERS OF GRAVITY

If US networks and computer systems are potential targets, there must be motives or "ends" that justify network attack "means". The problem for an adversarial state actor is what can be accomplished that will not generate vast counter-attacks from the United States. The first consideration to this is that a properly generated CNA may not have traceable "footprints". The second is that a small state actor may not care, particularly if it can justify its actions to the world community because the United States took military action against it, for whatever justifiable reason. The real issue, of course, is what could a state actor gain. Several possibilities are evident:

Economic Advantage-- actions taken to affect the availability and price of critical commodities such as oil, gas, industrial metals and all matters of food and their distribution systems. Such an economic advantage could give respective commodity producers significant market advantages over other nations including the US and its allies.

Psychological Paralysis-- measured sequential degradation of internal infrastructure could be used to generate powerful anti-war sentiment in the US, particularly if the US was involved in an excursion into the sovereignty of an adversary who is able to generate sympathy for its "defensive" actions. Actions against the banking and investment systems of the US would be particularly vulnerable to this if US stock and currency markets are seriously degraded due to their dependence on automation and computerization. In addition, any commercial enterprise dependent on Internet or "e-commerce" could be halted for indefinite periods of time, creating severe economic hardship. This same type of paralysis is feared as the "Y2K" problem approaches because of its largely unknown and unquantifiable potential impact.

Military Transportation and Logistics Degradation-- by causing disruptions of systems that limit movement on US-based rail, sea and air terminal operations, an adversary could seriously affect the ability of the United States to prosecute successfully actions in major regional conflicts or MRCs. Because the US military is highly dependent on command and administrative control systems to manage its transportation and logistics, the momentary disruption of selected underlying contracted private telecommunications could easily effect this degradation.

THE "PYRAMID OF VULNERABILITY" OF US INFRASTRUCTURE

Almost a year ago, the Army War College hosted its ninth annual strategy conference in Carlisle, Pennsylvania. This year the theme was "Challenging the United States Symmetrically and Asymmetrically: Can America Be Defeated?" One of the invited speakers was Robert David Steel, who went no further than to justify various US governmental initiatives that had already established momentum, including operations centers at the FBI and Ft. Meade[17]. Mr. Steel went on to state that the single existing US interagency initiative, the Presidents Commission on Critical Infrastructure Protection, or PCCIP, left the US "with no clear-cut direction, no one clearly in charge, and no basis for which to mobilize the private sector into its new and urgent role as the first line of national defense against cyber-attack and self-destructive electronic systems"[18]. Indeed, the entire effort has languished politically with various loosely coordinated individual agency efforts. Mr. Steel describes CNA vulnerabilities in terms of potential CNA objectives or targets in four distinct types of vulnerabilities[19]:

- Major physical infrastructure elements such as bridges, dams, canals, pipelines, and rail switching points.
- Obvious military "Achilles' Heels", such as submarine communications antennas, military sea departure channels, electrical power and communications supporting commands
- Vulnerability of core data streams such as military logistics, transportation status, financial accounts and financial transfers

- Vulnerability of the Intelligence Community to physical and cyber attacks against communications downlinks, Joint Intelligence Centers, global geo-spacial data.

THE OPEN NETWORK PROBLEM

The basic problem with defense of US network controlled facilities and commerce is the inherent lack of resiliency in network and computer systems. The vast majority of networks and computer systems in the United States are for the benefit of "for profit" enterprises, who must keep cost at a minimum in order to succeed. This contrasts with the development of the Internet, which was developed and originally funded by the US Government as ARPANET. This original "Internet" developed to be a largely redundant system that could provide a high degree of both reliability and availability of service due to its multiple routes and protocol design. Due to an extremely high rate of commercial extensions to this Internet, there now is a dependence on many parts of the Internet that have a "single thread" of connectivity without regard for back-up systems or networks. The "single thread" design means that there are multiple "weak links" in a sequential or serial network design, any one of which represents a "weak link" in the chain. The weak links could be either physical links that are vulnerable or redundant systems that because they were designed for significantly less traffic could be choke points in the event of the degradation of other routes in the network. The National Communications System agency recognizes this[20] and outlines many instances where the communications infrastructure of the United States has failed because lack of resiliency and redundancy. Critical communications nodes also exist that could easily be taken out of service creating service outages that would take at least days to relieve. Several years ago, a US telecommunications trade magazine reported on several of these key weak points and the vulnerabilities that they created. The cover of the magazine pictured the major eastern node of the Internet and where it was located in a pre-fabricated shelter in a parking garage near Washington, DC[21]. If selected critical communications systems in the United States are degraded significantly, there will be 2nd and 3rd order effects that create chaos for both the

computer systems and people that use them. However well that attacks against communications nodes and systems may perform, most damaging of all would be to leave communications systems alone, at least initially, and use these systems to access computer data and infrastructure performance through the communications systems.

ATTACK STRATEGIES

THE FOUR HORSEMEN OF CNA

There are several key means or techniques that CNA can be used to attack various levels and dependent systems controlled through the Global and Defense Information Infrastructure:

- Hacker CNA through open network architectures in the Internet or Intranets
- Hacker CNA through telephone network dial-up access
- Viruses distributed and accesses initiated through viruses
- Coercive embedded code

Guarding against each of these techniques requires a different approach at several different levels of an organization that uses the latest information technology. All require that Information Technology departments and local Network Administrators be trained and committed to implementing networks with safeguards and policies that inhibit CNA attacks.

THE ISO / OSI NETWORK MODEL AND VULNERABILITIES

The standard model for describing network elements and their interrelationships is the International Standards Organization's Open Systems Interconnect Model[22]. This ISO / OSI model is adhered to by network service providers, telecommunications common carriers as well as end-users such as private businesses, government and public systems. Seven layers are described;

each individually or as part of a technically coordinated attack in parallel could be the target of a CNA, as speculated here:

Layer 1 Physical -- a magnetic or electromechanical attack short of an actual physically destructive intrusion could affect the performance of this layer.

Layer 2 Data Link -- communications protocols, error checking and retransmissions can be affected by numerous techniques that could have the effect of overloading networks and degrading system performance sufficiently enough to cause system crashes and network failures.

Layer 3 Network -- network diagnostic systems within this layer of a network could be attacked resulting in error messages that could cause large scale network shut-downs or reroutes affecting network service performance.

Layer 4 Transport -- network addressing, spoofing or corruption of Internet protocol or IP network addresses can create both erroneous network messages, inquiries and responses that affect both the performance of networks as well as the messages placed on them.

Layer 5 Session -- shut-downs of session layer communications could be enabled through manipulation of IP packet inquiry or response as well as by the introduction of Java program applets and in session identification information found in cookies.

Layer 6 Presentation -- coercive imbedded programming code, introduced interactively or via initial manufacture into browsers could change or corrupt data responses or even affect local or wide area network performance by introducing viruses or coercive code into other layer functions.

Layer 7 Application -- viruses and other coercive imbedded code could be introduced at the application layer via downloads, back doors, Trojan horses and other techniques to thwart the effectiveness of anti-viral detection and correction programs.

THE CNA MULTIPLE DOMINO SCENARIO

The Domino Scenario may or may not require the combination with critical node and infrastructure physical attack, such as destruction of a key Internet router hub, telephone switching

point or power grid facility. Even if these sabotage or terrorism supporting attacks is not taken, the havoc that can be wrecked can be devastating. The attack could employ any or all of the following methodologies against varied targets that can create the combined effect of targeting directly the types of centers of gravity described earlier. The specific "battle order of attack" or sequencing each of these may depend upon a former application, or individually, each might stand alone against specific US targets in each of the following phases.

Pre-Crisis -- Targets for pre-crisis attack are networks of enterprises (including government systems), telephony and Internet operators:

Malicious and Embedded Software Introduced in link, network and application layer network-accessible software -- these software or firmware "bugs" would be triggered by a time event (a D-Day) or an if-then logic scenario. Presently identified techniques are known by various names: virus, worm, Trojan horse, time bomb, logic bomb, rabbit and bacterium[23].

ISR and Targeting -- An effective network attack depends upon up-to-the-minute reconnaissance to determine network points of attack, password vulnerabilities and to develop supporting attack plans[24]. Techniques employed here are spoofing, masquerading, sequential and dictionary scanning for password accesses, browsing and tunneling[25].

Sequential and Parallel CNAttacks – Attacks against enterprise networks, databases and intranet or Internet data and infrastructures would be undertaken with subsidiary networks attacked first to be followed by attacks against infrastructure capabilities such as transportation nodes, power grids and others using either Internet triggers or such external access as telephone maintenance ports on critical systems. Finally, the entire Internet could be disabled by a concerted attack on routers, switches and route databases. This could be surprisingly easy with various "overload" or spamming techniques, or could be quite sophisticated by actually attacking the route tables themselves.

The important point about this sequence of events is that it easily develops into a exponential effects chain, a pyramid of one effect causing a chain reaction to cause many more, potentially repeating many times over until irretrievable damage is done.

THE POLITICAL DILEMMA: FIRST AMENDMENT AND PRIVACY RIGHTS

The Domino Scenario does not take into account national borders or boundaries. In the mid-seventies, prior to the introduction of competition in the US and worldwide telephone systems, the telephone system carried modem-connected data from end-to-end through a system using dial-up or dedicated private channels with telephone company numbering that was easily traced from one end to the other. With the introduction of competition both domestically and abroad, there no longer is a single coordination authority that could be able to describe how a call or message is used to gain access over open network systems. The privacy advocates have a strong voice in American society most recently amplified by the uproar over the planned identification number engraved into the new Intel Pentium III microprocessor chip. Previously, the American Civil Liberties Union has been a vocal critic of various US executive and legislative efforts to actively promote the security of on-line commerce including the Clipper chip effort and key escrow. Recent ACLU testimony has been supportive of free trade provisions of the Pro-CODE (Promotion of Commerce On-line IN the Digital Era) Act of 1997[26].

CURRENT DEFENSE DOCTRINAL INITIATIVES

JOINT OPERATIONS INITIATIVES

Joint Vision 2010 provides the generalized doctrine for employment of information operations and concentrates on various general doctrinal pronouncements such as "information superiority"[27], "full spectrum dominance"[28], "full-dimensional protection"[29] and "battlespace awareness"[30]. These are all good initiatives but are only part of the overall Joint Vision 2010 approach to warfare, which depends heavily on specific information systems and accurate and timely intelligence and precise timely command and control communications. A recent speaker in

the Army War College's Commandant's Lecture Series stated that CINC, US SpaceCom would assume "primary responsibility" for information operations[31]. While this approach might focus all information operations under a single joint component, an unintended consequence could be that regional CINCs might not have an immediate direct interest in including the emerging and non-traditional information operations in the CINCs joint operations and theatre campaign plans, particularly regarding defenses against CNA.

SERVICE INITIATIVES

The Departments of the Air Force, Army and Navy each have developed joint and service- supporting initiatives in the sphere of information operations. The Air Force describes information operations as one of three new mission areas, which also includes counter-information and command and control attack. According to the Air Force, information operations is doctrinally broken out into the following mission areas: surveillance, command & control, communications, combat identification, reconnaissance, intelligence, weather and precision navigation[32]. The Navy doesn't have much readily available public information, but does have a publicly accessible description of its policy and doctrine relation to information security and the support that it provides its forces through its INFOSEC Technical Assistance Center in Charleston[33]. The Army has an evolving but comprehensive strategy and doctrine for the employment of information operations. The Army defines information operations as "Continuous military operations within the military information environment that enable, enhance, and protect the friendly force's ability to collect, process and act on information to achieve an advantage across the full range of military operations. Information operations include interacting with the global information environment and exploiting or degrading an adversary's information and decision capabilities"[34]. The Army's concept of land information warfare includes the following: "own the night, combat ID, extend the depth of precision fires, control information war, protect the force, digitize the battlefield"[35]. Each of these tenets depends on control and use of information and information technology. The Army has even initiated development of an information operations officer career field, as a result of its

OPMS XXI task force supporting JV 2010 and Force 21[36]. From these examples, it becomes obvious that each of the services is today defining its information operations needs for the year 2010 and Joint Vision 2010 in terms that each is comfortable with.

CURRENT DIFFUSION OF EFFORT

The diffusion of effort between each of the services is magnified by joint efforts that are being pursued and articulated via the joint doctrine and plans outlined earlier. The geographical CINCs are developing their own exercises and plans to employ information operations with little doctrinal guidance from the JCS. ACOM and PACOM have been the most aggressive player in joint information operations exercises, orchestrating the June, 1997 Eligible Receiver exercise as well as a follow-on exercise in 1998. Fortunately, in Eligible Receiver, significant help was provided from several other key national agencies such as the Joint Information Warfare Center in San Antonio and the National Security Agency. Much of this assistance was provided in the spirit of interagency cooperation and did not take place under specific statutory mandate. The CJCS staff provided overall coordination guidance to the exercise team[37].

STRUCTURAL DIFFICULTIES

The Scope of "Defensive Information" is too broad to allow for a meaningful discussion of ends, ways, means, strategy or force structure to exploit it. Everything requires information to function in the information age. The continued discussions that covers every imaginable aspect of information warfare, operations and defense diffuses the very efforts that are required to support the current critical requirement to concentrate on defenses against computer network attack. Everyone in the US Defense establishment needs to be concerned about how to protect its own information, telecommunications infrastructure and vital computer-based operations. This goes way beyond the concept of mere "information assurance". The management of information assurance, information operations and information warfare, whether offensive or defensive should

not be centralized but be decentralized to the "warfighter" The Prosecution of Information Operations and its brother in arms, Information Warfare is inseparable from the kinetic effects of military force and thus needs to be integrated with it at the geographical CINC level. This will have the effect of separating computer network attack defense to be handled on a localized basis, throughout not just DoD but throughout the government and in cooperation with industry.

The most vulnerable dimension of the information defense of the US is not the vulnerability of elements of the US Department of Defense to Information Warfare Attack. The greatest vulnerability is that of the US Information Architecture itself, which is operated and maintained by the largely civilian private sector. The next greatest vulnerability is those infrastructure points that rely to a great extent on accurate information and the assurance of accurate information to operate them.

RECOMMENDATIONS

There probably will not be any quick solutions to putting defense against information operations on a clear and successful track for development and success. There are too many potentially competing centers of power in the DoD, as well as in the larger US government. Each of the intelligence agencies, the JCS, military services, NIST and the civilian law enforcement agencies such as the FBI, all have roles in various aspects of the defensive part of information operations. Fortunately, each of these centers appears to be developing its position and expertise in the information operations arena independently. As a result of the ambiguity of the current problem and the potential threat of disaster, there probably cannot be an "either-or" approach to courses of action to prepare for the world of 2010. The largest problem to prevent significant new activity at the DoD or JCS level is the lack of individual agency funding and the requisite statutory authority for every agency of government to be individually responsive and responsible for defense against potential computer network attacks against US infrastructure. Secretary Cohen has

already set the stage for what could be needed private sector relationships and partnerships in research, development and continued emphasis on protection and defense vigilance.// It's important however, to ensure that every agency in the federal and more largely, state governments, take on an independent initiative to guard against CNA. The tendency of the US federal government and even the Department of Defense separately, to centralize various aspects and functions of this potential threat into an overall coordinating authority should be resisted. Only when every agency of government takes on the direct responsibility for vigilance against CNA individually will the United States be able to appropriately arrest the complex and far-reaching effects of these potential attacks.

Word Count = 5,282

ENDNOTES

[1] Reuters PLC, News Report; available from <http://dailynews.yahoo.com/headlines/ts/story.html?s=v/nm/19990228/ts/hackers_1.html>. Internet; accessed 28 February 1999.

[2] These paraphrased statements are based upon remarks made by speakers (under an AWC non-attribution policy) participating in the AWC Commandant's Lecture Series, AWC noontime lectures and other AWC lectures in Dec 1998 - Jan 1999.

[3] Senator Jon Kyle. Press Release "Military Computer Hackers Eluded Identification for Four Days During February Gulf Tensions, Kyl Panel Told", 10 June 1998; available from <http://www.senate.gov/~Kyl>. Internet; accessed 9 September 1998.

[4] Ibid.

[5] William S. Cohen, Secretary of Defense, Report of the Quadrennial Defense Review. Washington, May 1997. 37.

[6] Alvin and Heidi Toffler, War and Anti-War. New York: Warner Books, 1993.

[7] John L. Petersen, The Road to 2015: Profiles of the Future. Corte Madera, CA, 1994.

[8] Henry Ryan and C. Edward Peartree. Military Theory and Information Warfare. 123.

[9] The White House, A National Security Strategy for a New Century. May, 1997, 14.

[10] Ibid., 76.

[11]Congress of the United States Bill Summary and Status available from <http://thomas.loc.gov/cgi-bin/bdquery/z?d105:HRO1903:@@@L>; Internet; accessed 12 January 1998.

[12] William S. Cohen, Remarks prepared for delivery to Microsoft Corporation employees in Redmond, Washington, on Thursday, February 18, 1999; US Department of Defense: Armed Forces Information Service: Defense Viewpoint, available from <http://www.defenselink.mil/speeches/1999/s19990218-secdef.html>; Internet; accessed 28 February, 1999.

[13] Martin Libicki, NDU - 1995; available from <http://www.ndu.edu/ndu/inss/actpubs/act003>; Internet; accessed 9 September 1998.

[14] Ibid.

[15] Robert Minehart. Information Warfare Tutorial. Carlisle, PA, US Army War College, Center for Strategic Leadership available from <http://www.carlisle-awc.mil/usucls/org/iw/tutorial/mod10.htm>. Internet. Accessed on 12 October 1998.

[16] Ibid. /mod6.htm.

[17] Robert David Steel, "Takedown, Tools, & Technocracy" Final Draft paper presented at the Ninth Annual Strategy Conference, US Army War College, 31 March 1998; available from <http://www.fas.org/irp/eprint/takedown1.htm>; Internet; accessed 9 October 1998.

[18] Ibid.

[19] Ibid.

[20] National Communications System: Leadership Excellence in Technology, 35th Anniversary Book, Defense Information Systems Agency, DC. 1998 -- the National Communications System is a joint civilian and government steering agency under the administrative support of the Defense Information Systems Agency.

[21] Discovered by the author in work he performed for his USAF Reserve assignment. The article is not referenced here because of its sensitivity.

[22] ITU ISO / OSI Network Model; available from Http://linus.ucs.indiana.edu/usail/network/nfs/network_layers.html>; Internet; accessed on 2 Feb 1999.

[23] Questech, Inc. Computer Security Threats Chart, Falls Church, VA, Sep 1997.

[24] Jeremy Singer, Inside the Army , December 21, 1998 describes vividly these techniques demonstrated by Philip Loranger, in briefings given to DoD and Dept of the Army executives.

[25] Questech, Inc. Computer Security Threats Chart, Falls Church, VA, Sep 1997.

[26] American Civil Liberties Union. Cyber-Liberties: available from http://www.aclu.org/issues/cyber/priv/pro.rtf.html>; Internet; accessed on 27 Dec 1998.

[27] Department of Defense, Joint Chiefs of Staff, Concept for Future Operations: Expanding Joint Vision 2010. (Joint Warfighting Center, Ft. Monroe, VA). 1997. 35.

[28] Ibid. 51.

[29] Ibid. 52.

[30] Ibid. 83.

[31] This statement is based upon remarks made by a speaker (under an AWC non-attribution policy) participating in the AWC Commandant's Lecture Series.

[32] US Air Force Fact Sheet; available from <http://www.af.mil/news/factsheets/InformationWarfare.html>; Internet; accessed on 11 October 1998.

[33] US Navy Systems Center. Homepage for the INFOSEC Technical Assistance Center available from <http://infosec.nosc.mil/content.html; Internet; accessed on 12 October 1998.

[34] Minehart, Robert. Information Warfare Tutorial. /mod8hl.htm#army.

[35] Ibid.

[36] "FA 30-Information Operations" Officer Career Field; available from <http://www.army.mil/opms/Fa30.htm>; Internet; accessed 9 September 1998.

[37] Author's notes from experiences gained at his USAF reserve assignment.

BIBLIOGRAPHY

Alberts, David S. Defensive Information Warfare. Washington, DC, National Defense University, 1996.

Cohen, William S., Secretary of Defense. Annual Report to the President and the Congress. U.S. Government Printing Office, 1998.

Cohen, William S., Secretary of Defense, Report of the Quadrennial Defense Review. Washington, May 1997.

Henry, Ryan and C. Edward Peartree. "Military Theory and Information Warfare" Parameters 28 -- no. 3 (Autumn 1998): 121-135.

Johnson, Stuart E. and Martin Libicki, Ed. Dominant Battlespace Knowledge. Washington, DC, National Defense University. 1995.

Kyle, Jon: US Senator. Press Release "Military Computer Hackers Eluded Identification for Four Days During February Gulf Tensions, Kyl Panel Told", 10 June 1998; Available from <http://www.senate.gov/~Kyl>. Internet; accessed 9 September 1998.

Libicki, Martin. What is Information Warfare?. Washington, DC, National Defense University, 1995.

Lykke, Arthur F. "Toward an Understanding of Military Strategy" Vol I Readings, Course 2: "War, National Policy & Strategy". Army War College, 1998.

Minehart, Robert. "Information Warfare Tutorial". Carlisle, PA, US Army War College, Center for Strategic Leadership available from <http://www.carlisle-awc.mil/usucls/org/iw/tutorial/mod10.htm>. Internet. Accessed on 12 October, 1998.

National Communications System: Leadership Excellence in Technology, 35th Anniversary Book, Defense Information Systems Agency, DC. 1998.

Questech, Inc. Computer Security Threats Chart, Falls Church, VA, Sep 1997.

Steel, Robert David. "Takedown, Tools, & Technocracy" Final Draft paper presented at the Ninth Annual Strategy Conference, US Army War College, 31 March 1998; Available from <http://www.fas.org/irp/eprint/takedown1.htm>; Internet; accessed 9 October 1998.

Toffler, Alvin and Heidi. War and Anti-War. New York: Warner Books, 1993.

The White House. A National Security Strategy for a New Century. May, 1997.

US Air Force Fact Sheet 95-20. "Information Warfare"; Available from <http://www.af.mil/news/factsheets/Information_Warfare.html>; Internet; accessed 11 October, 1998.

US Army. Career "Functional Area 30-- Information Operations"; Available from <http://www.army.mil/opms/Fa30.htm>; Internet; accessed 8 September 1998.

U.S. Army War College, Communicative Arts Program Directive, AY99. Carlisle Barracks: U.S. Army War College, 1998.

US Department of Defense, Joint Chiefs of Staff, Concept for Future Operations: Expanding Joint Vision 2010. Joint Warfighting Center, Ft. Monroe, VA. 1997.

US Department of Defense, Joint Chiefs of Staff, Information Assurance: Legal, Regulatory, Policy and Organizational Considerations, 3rd Edition. J6, The Pentagon, Washington, DC. 17 September1997.